Cerri Enterprise Collaboration Software Security Overview

Built for Security

Product Information & Sales
Call us at +1-866-877-4364
www.cerri.com

Security is one of the founding pillars of Cerri Enterprise Apps and plays an intrinsic role in the development process of the software. Cerri safeguards your data from any intrusions, ensuring its availability, integrity and confidentiality are protected.

Cerri upholds AWS' shared responsibility model with respect to compliance across its data-locations.

System Access

- You are responsible for granting and revoking access to users across your Cerri instance.
- Single page sign on and advanced data encryption mean your account and data are protected from outside intrusion during transit. (Your encrypted login data is transmitted via TSL (new SSL) or HTTPS port/443).

Managed Access to Data

- Cerri API validates user access to all data based on permissions.
- Users only see data they have been authorized to view by project owners.
- Admin users may revoke or reinstate users from the instance as a whole at any time.

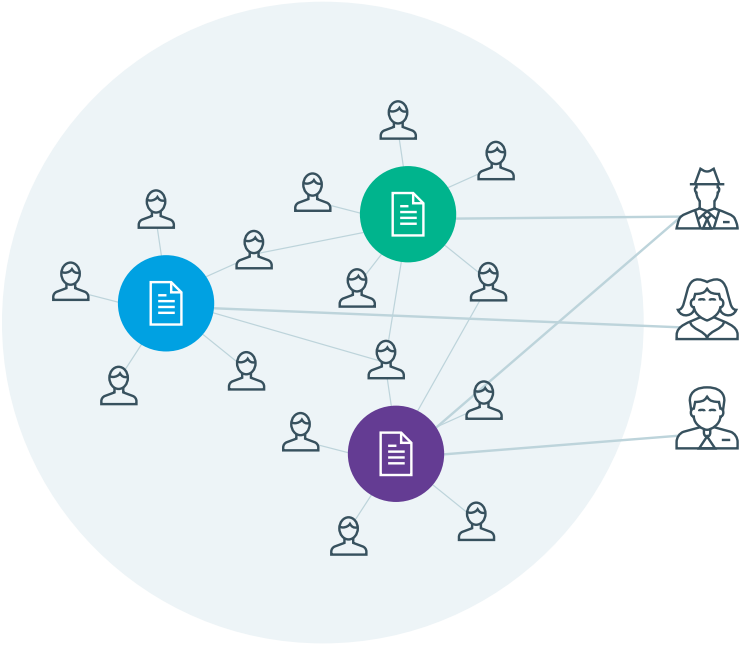
Continuous Permission Monitoring

- Cerri uses strong user authentication for every request to the instance.
- Unlike systems which authenticate at login or at the system level, Cerri defines permissions at the item level.
- On every request to the API we verify that users are properly authenticated, have a valid license and have the appropriate rights to perform the request.

Projects and Files

- All Cerri users, except those with limited access, may create projects and share them with other users within your instance.
- Project permissions are designed to enable specific project collaboration activities: Edit, Create, View only and Guest permission-levels are established at project-level and allow project-members to view, create and edit tasks, upload and download files inside the project, and comment.
- The project-owner can change permission-level or revoke access from any project-member at any time without removing that user from the instance as a whole.

Strict Project Permission Levels



No Public Linking

- Cerri does not enable users to link any item in the instance to webpages, blogs, or other third-party software.
- Link-sharing requires that users log in by default.
- Guest-permission level enables users from outside the instance such as clients and suppliers to view and complete tasks and attach files in projects they are invited to without being able to see the rest of the project content, files or members.

Data Centre Security

- You select the region(s) in which your content will be stored.
- Your data centre location is determined by the first admin user's location.
- Cerri does not relocate or replicate your content outside of your chosen region(s), except as legally required and as necessary to maintain your services.
- Our Amazon data centers are located in Germany and in North Virginia.
- Cerri complies with the European Union Security Standards; providing you with maximum data protection.

Database Security & Reliability

- Cerri runs on PostgreSQL, the award-winning open source database.
- PostgreSQL offers an uncompromising stability which safeguards from any inconsistencies or loss of data in case of system or power failures.

No Search Engine indexing

- Cerri prevents indexing of data stored in Cerri by search engines or robots.